TLP: WHITE

Disclosure is not limited. Subject to standard copyright rules, TLP: WHITE information may be distributed without restriction.

http://www.us-cert.gov/tlp/

DATE(S) ISSUED:
10/16/2019

SUBJECT:
Oracle Quarterly Critical Patches Issued October 15, 2019

OVERVIEW:
Multiple vulnerabilities have been discovered in Oracle products, which could allow for remote code execution.

SYSTEMS AFFECTED:

- Agile Recipe Management for Pharmaceuticals, versions 9.3.3, 9.3.4
- Diagnostic Assistant, version 2.12.36
- Enterprise Manager Base Platform, versions 13.2, 13.3
- Enterprise Manager for Exadata, versions 12.1.0.5.0, 13.2.2.0.0, 13.3.1.0.0, 13.3.2.0.0
- Enterprise Manager Ops Center, versions 12.3.3, 12.4.0
- Fujitsu M10-1, M10-4, M10-4S, M12-1, M12-2, M12-2S Servers, versions prior to XCP2361, prior to XCP3071
- Hyperion Data Relationship Management, version 11.1.2.4
- Hyperion Enterprise Performance Management Architect, version 11.1.2.4
- Hyperion Financial Reporting, version 11.1.2.4
- Instantis EnterpriseTrack, versions 17.1, 17.2, 17.3
- JD Edwards EnterpriseOne Tools, version 4.0.1.0
- MICROS Relate CRM Software, versions 7.1.0, 11.4, 15.0.0, 16.0.0, 17.0.0, 18.0.0
- MICROS Retail XBRi Loss Prevention, version 10.8.3
- MySQL Connectors, versions 5.3.13 and prior, 8.0.17 and prior
- MySQL Enterprise Monitor, versions 8.0.17 and prior
- MySQL Server, versions 5.6.45 and prior, 5.7.27 and prior, 8.17 and prior
- MySQL Workbench, versions 8.0.17 and prior
- Oracle Agile PLM, versions 9.3.3-9.3.6
- Oracle Agile Product Lifecycle Management for Process, versions 6.2.0.0, 6.2.1.0, 6.2.2.0, 6.2.3.0
- Oracle API Gateway, version 11.1.2.4.0
- Oracle Application Testing Suite, versions 13.2, 13.3
- Oracle Banking Digital Experience, versions 18.1, 18.2, 18.3, 19.1
- Oracle Banking Platform, versions 2.4.0, 2.4.1, 2.5.0, 2.6.0, 2.6.1, 2.7.0, 2.7.1
- Oracle BI Publisher, versions 11.1.1.9.0, 12.2.1.3.0, 12.2.1.4.0
- Oracle Business Intelligence Enterprise Edition, versions 11.1.1.9.0, 12.2.1.3.0, 12.2.1.4.0

- Oracle Clusterware, version 19.0.0.0.0
- Oracle Data Integrator, version 12.2.1.3.0
- Oracle Database Server, versions 11.2.0.4, 12.1.0.2, 12.2.0.1, 18c, 19c
- Oracle E-Business Suite, versions 12.1.1-12.1.3, 12.2.3-12.2.9
- Oracle Enterprise Repository, version 12.1.3.0.0
- Oracle Financial Services Analytical Applications Infrastructure, versions 8.0.2-8.0.8
- Oracle Financial Services Enterprise Financial Performance Analytics, versions 8.0.6, 8.0.7
- Oracle Financial Services Retail Performance Analytics, versions 8.0.6, 8.0.7
- Oracle FLEXCUBE Direct Banking, versions 12.0.2, 12.0.3
- Oracle Forms, version 12.2.1.3.0
- Oracle GoldenGate Application Adapters, version 12.3.2.1.0
- Oracle GraalVM Enterprise Edition, version 19.2.0
- Oracle Healthcare Foundation, versions 7.1.1, 7.2.2
- Oracle Healthcare Translational Research, versions 3.1.0, 3.2.1, 3.3.1
- Oracle Hospitality Cruise Dining Room Management, version 8.0.80
- Oracle Hospitality Guest Access, versions 4.2.0, 4.2.1
- Oracle Hospitality Materials Control, version 18.1
- Oracle Hospitality Reporting and Analytics, version 9.1.0
- Oracle Hospitality RES 3700, version 5.7
- Oracle Java SE, versions 7u231, 8u221, 11.0.4, 13
- Oracle Java SE Embedded, version 8u221
- Oracle JDeveloper and ADF, versions 11.1.1.9.0, 11.1.2.4.0, 12.1.3.0.0, 12.2.1.3.0
- Oracle NoSQL Database, versions prior to 19.3.12
- Oracle Outside In Technology, version 8.5.4
- Oracle Policy Automation, versions 10.4.7, 12.1.0, 12.1.1, 12.2.0-12.2.15
- Oracle Policy Automation Connector for Siebel, version 10.4.6
- Oracle Policy Automation for Mobile Devices, versions 12.2.0-12.2.15
- Oracle Retail Customer Insights, versions 15.0, 16.0
- Oracle Retail Customer Management and Segmentation Foundation, version 17.0
- Oracle Retail Integration Bus, versions 15.0, 16.0
- Oracle Retail Xstore Office, version 7.1
- Oracle Retail Xstore Point of Service, versions 7.1, 15.0, 16.0, 17.0, 17.0.3, 18.0, 18.0.1, 19.0.0
- Oracle Service Bus, versions 11.1.1.9.0, 12.1.3.0.0, 12.2.1.3.0
- Oracle SOA Suite, version 12.2.1.3.0
- Oracle Solaris, versions 10, 11
- Oracle Virtual Directory, version 11.1.1.9.0
- Oracle VM VirtualBox, versions prior to 5.2.34, prior to 6.0.14
- Oracle Web Services, version 12.2.1.3.0
- Oracle WebCenter Portal, version 12.2.1.3.0
- Oracle WebLogic Server, versions 10.3.6.0.0, 12.1.3.0.0, 12.2.1.3.0
- PeopleSoft Enterprise HCM Human Resources, version 9.2
- PeopleSoft Enterprise PeopleTools, versions 8.56, 8.57
- PeopleSoft Enterprise SCM eProcurement, version 9.2
- Primavera Gateway, versions 15.2, 16.2, 17.12, 18.8
- Primavera P6 Enterprise Project Portfolio Management, versions 15.1.0-15.2.18, 16.1.0-16.2.18, 17.1.0-17.12.14, 18.1.0-18.8.13

- Primavera Unifier, versions 16.1, 16.2, 17.7-17.12, 18.8
- Siebel Applications, versions 19.8 and prior

RISK:
Government:

- Large and medium government entities: **High**
- Small government entities: **High**

Businesses:

- Large and medium business entities: **High**
- Small business entities: **High**

Home users: Low

RECOMMENDATIONS:
The following actions should be taken:

- Apply appropriate patches provided by Oracle to vulnerable systems immediately after appropriate testing.
- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.
- Remind users not to visit websites or follow links provided by unknown or untrusted sources.
- Inform and educate users regarding the threats posed by hypertext links contained in emails or attachments especially from un-trusted sources.
- Apply the Principle of Least Privilege to all systems and services.

REFERENCES:
Oracle:
https://www.oracle.com/technetwork/security-advisory/cpuoct2019-5072832.html

TLP: WHITE
Disclosure is not limited. Subject to standard copyright rules, TLP: WHITE information may be distributed without restriction.
http://www.us-cert.gov/tlp/

This message and attachments may contain confidential information. If it appears that this message was sent to you by mistake, any retention, dissemination, distribution or copying of this message and attachments is strictly prohibited. Please notify the sender immediately and permanently delete the message and any attachments.

Chris Watts
Security Operations Analyst
MS Department of Information Technology Services
601-432-8201 | www.its.ms.gov

iTS Mississippi Department of
Information Technology Services
3771 Eastwood Drive | Jackson, Mississippi 39211-6381

DISCLAIMER: This email and any files transmitted with it are confidential and intended solely for the use of the individual or entity to whom they are addressed. If you have received this email in error please notify the system manager. This message contains confidential information and is intended only for the individual named. If you are not the named addressee you should not disseminate, distribute or copy this e-mail. Please notify the sender immediately by e-mail if you have received this e-mail by mistake and delete this e-mail from your system. If you are not the intended recipient you are notified that disclosing, copying, distributing or taking any action in reliance on the contents of this information is strictly prohibited